



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1440  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,797	05/22/2001	Thomas L. Gindin	POU920010018US1	1174
7590	03/09/2006		EXAMINER [REDACTED]	SON, LINH L D
Sean F. Sullivan Cantor Colburn LLP 55 Griffin Road South Bloomfield, CT 06002		ART UNIT [REDACTED]		PAPER NUMBER 2135

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/862,797	GINDIN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 12/07/05.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1,2,5-9,12-16 and 19-24 is/are rejected.
- 7) Claim(s) 3,4,10,11,17 and 18 is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_.

**DETAILED ACTION**

1. This Office Action is responding to the Amendment received on 12/07/05.
2. Claims 1-24 are pending.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-2, 5-9, 12-16, and 19-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent, US Patent No. 6671804B1 (See PTO-892 filed on 12/12/04, in view of Sudia, US Publication No. 20050114666A1.

5. As per claims 1, 8, 15, and 22-24, Kent discloses "A method for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, the method comprising: receiving, from the certification authority in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the identity of the end user, and a proof of identity possession by the end user" in (Col 7 lines 1-35, Col 9

lines 35-60, Col 9 line 60 to Col 10 line 40 (private Key is the proof of identity possession)); “analyzing the content of said plurality of data fields; verifying the accuracy of said plurality of data fields; and if said plurality of data fields is verified as accurate, sending a signed object to the certification authority, said signed object comprising the proof of possession confirmation” in (Col 10 lines 25-40, Col 7 lines 1-35, Col 8 lines 23-45, Col 9 lines 15-28, and Col 12 lines 25-48). However, Kent is silent on the limitation “said proof of possession confirmation is constructed in a manner so as to prevent replay attacks by an imposter”. Nevertheless, Sudia discloses “Blocked Tree Authorization and Status Systems” invention, which includes an authentication method for requesting an attribute certificate that comprises multiple fields, and a hash string, which is utilized to authenticate and proof of possessing the certificate (Para 0072, 0085, 0087, 0111-0128, 0238-239, 0256, and 0329-342). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Kent’s invention to incorporate hash string of information as a key to encrypt the requesting object fields with the motivation of strengthening the authentication security.

6. As per claims 2, 9, and 16, Kent discloses “the method of claims 1, 8, and 15, wherein said plurality of data fields further comprises: a host name; a subject identification; a subject public key information; and a sealed proof of possession” in (Col 7 lines 1-35, Col 9 lines 35-60, Col 9 line 60 to Col 10 line 40, and Col 12 lines 25-48 (private Key is the proof of identity possession) (extension field can be used to include

the host name info)).

7. As per claims 5-6, 12-13, and 19-20, Kent discloses "the method of claims 3 and 10, wherein said extracted password and said extracted key identifier are initially symmetrically encrypted" in (Col 10 lines 25-40). It is well known in the art that the X.509 certificate utilizes symmetrical and asymmetrical encryption utilizing private-public key.
8. As per claims 7, 14, and 21, Claim 1 rejection basis is incorporated. Further, Kent discloses "the method of claims 1 and 8, wherein: said plurality of data fields includes a password; and said signed object does not include said password" in Sudia (Para 0072, 0085, 0087, 0111-0128, 0238-239, 0256, and 0329-342).

#### ***Response to Arguments***

9. Applicant's arguments filed 12/07/05 have been fully considered but they are not persuasive.
10. On page 9 of the remark, Applicant argues that Sudia reference does not in fact provide the capability of preventing replay attacks by an impostor. Examiner disagrees with the Applicant completely. In Para 0085, and 0087, Sudia discloses clearly a

method of utilizing a hash string of values, such as certificate number, validity period, issuer name, and etc., to validate the certificate. The validity period variable in the string of values will definitely prevent the replay attacks by an impostor. Therefore, it is clearly that Sudia fully discloses the proof of possession confirmation limitation.

Therefore, the rejection basis dated 09/07/05 is maintained.

***Allowable Subject Matter***

11. Claims 3-4, 10-11, 17-18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100